



A Review On Hybrid Intrusion Detection System Using Svm For Anomaly And Misuse Detection In Networks

¹Monika Rokde, ²Goldy Saini, ³Swati Khanve, ⁴Nitya Khare

¹M.tech scholar, ²Asst. Prof., ³Asst. Prof., ⁴Asst. Prof. & HOD

Dept. Of Computer Science & Engineering,

Sagar Institute of Research and Technology-Excellence, Bhopal, India

Abstract: Intrusion Detection Systems (IDS) are essential for protecting networks from cyber threats. Traditional IDS methods, including anomaly-based and misuse-based detection, have limitations such as high false positive rates and inability to detect novel attacks. A hybrid IDS combines both techniques to enhance accuracy and efficiency. Support Vector Machines (SVM) have proven to be effective in classifying network traffic for intrusion detection. This paper reviews the application of SVM in hybrid IDS, its advantages, challenges, and potential improvements for network security.

Index Terms - Intrusion Detection Systems, support vector machine, anomaly detection, Denial-of-Service (DoS), network traffic.

I. INTRODUCTION

As the digital landscape continues to expand, cyber threats are becoming increasingly sophisticated, posing significant challenges to organizations and individuals alike. The proliferation of network-based attacks, such as Denial-of-Service (DoS), phishing, malware, and zero-day exploits, necessitates the development of robust security mechanisms to safeguard sensitive information and critical infrastructure. Traditional security measures, such as firewalls and antivirus software, are no longer sufficient to combat evolving cyber threats, as attackers continuously devise new techniques to bypass static defenses. Consequently, Intrusion Detection Systems (IDS) have emerged as a critical component in network security, offering proactive threat detection by monitoring network traffic for signs of malicious activity.

IDSs operate by analyzing patterns and behaviors in network data to identify potential intrusions. However, traditional IDS approaches suffer from limitations. Signature-based detection (misuse detection) relies on predefined attack signatures, making it ineffective against novel attacks. Meanwhile, anomaly-based detection, which flags deviations from normal behavior, often generates high false alarm rates due to its inability to distinguish between legitimate but unusual activities and actual intrusions. To overcome these challenges, hybrid IDSs have been developed, combining the strengths of both anomaly-based and misuse-based detection techniques. By integrating these two approaches, hybrid IDSs aim to improve detection accuracy, reduce false positives, and enhance overall network security.

Among the various machine learning techniques applied in IDS, Support Vector Machines (SVM) have demonstrated promising results. SVM is a supervised learning algorithm that excels in classification tasks, making it highly effective for both anomaly and misuse detection. It can learn complex decision boundaries and adapt to evolving attack patterns, thereby improving the overall efficiency of intrusion detection. Given these advantages, this review focuses on hybrid IDSs that leverage SVM for anomaly and misuse detection in networks, examining their effectiveness, challenges, and future directions.

Objectives of the Review

The primary objective of this review is to provide a comprehensive analysis of hybrid Intrusion Detection Systems that utilize Support Vector Machines for anomaly and misuse detection. Specifically, the review aims to:

1. **Examine the limitations of traditional IDS approaches** – This includes understanding the weaknesses of purely signature-based and purely anomaly-based detection techniques.
2. **Explore the role of hybrid IDSs** – The review investigates how hybrid IDSs integrate anomaly and misuse detection to enhance overall security and detection accuracy.
3. **Analyze the application of SVM in IDS** – The effectiveness of SVM in detecting network anomalies and known attack signatures is assessed.
4. **Discuss performance evaluation metrics** – Various performance metrics such as accuracy, precision, recall, and F1-score are reviewed to compare SVM-based IDS with other techniques.
5. **Identify research gaps and future directions** – The review highlights the challenges faced by SVM-based hybrid IDS and explores potential improvements for future research.

1.1 Overview of IDS and Its Significance

An Intrusion Detection System (IDS) is a security mechanism designed to monitor and analyze network traffic for signs of malicious activities or policy violations. IDSs are broadly classified into two categories: **Network-based Intrusion Detection Systems (NIDS)** and **Host-based Intrusion Detection Systems (HIDS)**. NIDS monitors network traffic for suspicious activities, whereas HIDS analyzes logs and activities on individual devices to detect potential threats.

The importance of IDS in cybersecurity cannot be overstated. With the increasing volume and sophistication of cyberattacks, organizations require automated and intelligent systems to detect and respond to intrusions in real time. Traditional security solutions, such as firewalls and access control mechanisms, primarily focus on preventing unauthorized access but often fail to detect sophisticated attacks that exploit vulnerabilities within the network. IDS acts as a second line of defense by identifying and mitigating potential threats before they escalate into major security breaches.

1.2 FUNDAMENTALS OF INTRUSION DETECTION SYSTEMS (IDS)

An Intrusion Detection System (IDS) is a security mechanism designed to monitor and analyze network traffic or system activities to detect unauthorized access, malicious activities, or policy violations. IDS functions as a surveillance tool that identifies potential security breaches by inspecting data packets, user behaviors, and system logs. Unlike firewalls, which primarily prevent unauthorized access, IDS works as a **detection system** that alerts administrators when an attack or anomaly is detected. IDS can operate in real-time to identify threats as they occur or analyze historical data to uncover patterns of intrusion.

1.3 IMPORTANCE IN NETWORK SECURITY

With the increasing sophistication of cyber threats, IDS has become an essential component of modern network security. Cyberattacks such as malware infections, denial-of-service (DoS) attacks, unauthorized access attempts, and insider threats can cause significant financial and operational damage. IDS helps organizations **proactively detect and mitigate security breaches**, minimizing the risk of data theft, service disruptions, and system compromise. Moreover, IDS provides valuable insights for security teams by logging attack details, allowing them to refine their security policies and improve defense mechanisms. It also enhances compliance with regulatory frameworks by ensuring continuous monitoring and reporting of suspicious activities.

1.4 TYPES OF IDS

IDSs are broadly categorized into three main types: **Anomaly-based IDS**, **Misuse-based IDS**, and **Hybrid IDS**. Each type has its strengths and weaknesses, making them suitable for different cybersecurity needs.

1. Anomaly-based IDS

Anomaly-based IDS identifies deviations from established normal behavior within a network or system. It relies on statistical models, machine learning algorithms, or heuristics to detect unusual activities that may indicate a security threat. This approach is effective in identifying **zero-day attacks and novel threats** that

do not have predefined signatures. However, anomaly-based IDS tends to generate **high false positive rates** because legitimate but uncommon activities may be mistakenly flagged as intrusions.

2. Misuse-based IDS (Signature-based IDS)

Misuse-based IDS detects intrusions by comparing incoming network traffic or system activities against a database of known attack signatures. It is highly effective at recognizing previously identified threats with a high degree of accuracy. This method is widely used in commercial IDS solutions due to its low false positive rate. However, **its major drawback is its inability to detect new, unknown, or zero-day attacks** since it relies on predefined signatures that must be regularly updated.

3. Hybrid IDS

Hybrid IDS combines the advantages of both anomaly-based and misuse-based approaches to improve detection accuracy and reduce false positives. By leveraging **anomaly detection** to identify unknown attacks and **misuse detection** to recognize known threats, hybrid IDS enhances network security by providing a more **comprehensive and adaptive detection mechanism**. This approach is increasingly being adopted in modern cybersecurity solutions, especially with the integration of **machine learning techniques such as Support Vector Machines (SVM), deep learning, and artificial intelligence**, to improve intrusion detection efficiency.

II. LITERATURE REVIEW

In [1], work is based on the enhancement of the highest Detection Rate (DR) algorithm which is Linear Genetic Programming (LGP) reducing the False Alarm Rate (FAR) incorporates with Bees Algorithm. Finally, Support Vector Machine (SVM) is one of the best candidate solutions to settle IDSs problems. In this study, four sample dataset containing 4000 random records are excluded randomly from this dataset for training and testing purposes. Experimental results show that the LGP_BA method improves the accuracy and efficiency compared with the previous related research and the feature subcategory offered by LGP_BA gives a superior representation of data [1]. In [2]; the authors propose a new approach of combining SVM and Bee Colony to achieve high quality performance of IDS. Their algorithm is implemented and evaluated using a standard benchmark KDD99 dataset. Experimental results show that SVM with Bee colony achieves an average accuracy is 88.46% [2]. In [3], a new hybrid intrusion detection method that hierarchically integrates a misuse detection model and an anomaly detection model in a decomposition structure is proposed. First, a misuse detection model is built based on the C4.5 decision tree algorithm and then the normal training data is decomposed into smaller subsets using the model. Next, multiple one-class SVM models are created for the decomposed subsets. As a result, each anomaly detection model does not only use the known attack information indirectly but also builds the profiles of normal behavior very precisely. The proposed hybrid intrusion detection method was evaluated by conducting experiments with the NSL-KDD data set. The experimental results demonstrate that the proposed method is better than the conventional methods in terms of the detection rate for both unknown and known attacks while it maintains a low false positive rate. In addition, the proposed method significantly reduces the high time complexity of the training and testing processes. Experimentally, the training and testing time of the anomaly detection model is shown to be only 50% and 60%, respectively, of the time required for the conventional models [3]. In [4], the authors proposed a hybrid approach toward achieving a high detection rate with a low false positive rate. The approach is a two level hybrid solution consisting of two anomaly detection components and a misuse detection component. In stage 1, an anomaly detection method with low computing complexity is developed and employed to build the detection component. The k-nearest neighbor's algorithm becomes crucial in building the two detection components for stage 2. In this hybrid approach, all of the detection components are well-coordinated. The detection component of stage 1 becomes involved in the course of building the two detection components of stage 2 that reduce the false positives and false negatives generated by the detection component of stage 1. Experimental results on the KDD99 dataset and the Kyoto University Benchmark dataset confirm that the proposed hybrid approach can effectively detect network anomalies with a low false positive rate [4]. In [5], an intrusion detection algorithm based on the AdaBoost algorithm was proposed. In the algorithm, decisions are used as weak classifiers. The decision rules are provided for both categorical and continuous features. By combining the weak classifiers for continuous features and the weak classifiers for categorical features into a strong classifier, the relations between these two different types of features are handled naturally, without any forced conversions between continuous features. Adaptable initial weights and a simple strategy for avoiding overfitting are adopted to improve the performance of the algorithm. Experimental results show that this algorithm has low computational complexity and error rates, as compared with algorithms of higher computational complexity, as tested on the benchmark sample data [5]. In [6], the proposed method uses a

training set of KDD-Cup99. The proposed method uses three main learning algorithms, SVM, Naive Bayes and the J48 decision tree is implemented and evaluated separately. These algorithms are also implemented and evaluated individually as well. The results show the superiority of the proposed method with 97% efficiency using J48 learning algorithm and AdaBoost classification by reducing the dimension IG method [6]. In [7], a technique based on the Online Sequential Extreme Learning Machine (OS-ELM) is presented for intrusion detection. The proposed technique uses alpha profiling to reduce the time complexity while irrelevant features are discarded using an ensemble of filtered, correlation and consistency based feature selection techniques. Instead of sampling, beta profiling is used to reduce the size of the training dataset. For performance evaluation of proposed technique, the standard NSL-KDD 2009 (Network Security Laboratory-Knowledge Discovery and DataMining) dataset is used. In this paper time and space complexity of the proposed technique is also discussed. The experimental results yielded an accuracy of 98.66% with a false positive rate of 1.74% and a detection time of 2.43 s for binary class NSL-KDD dataset. The proposed IDS achieve 97.67% of accuracy with 1.74% of the false positive rate in 2.65 s of detection time for the multi-class NSL-KDD dataset. The Kyoto University benchmark dataset is also used to test the proposed IDS. The accuracy of 96.37% with a false positive rate of 5.76% is yielded by the proposed technique. The proposed technique outperforms other published techniques in terms of accuracy, false positive rate and detection time. Based on the results, it is concluded that the proposed method is an efficient method for detecting network intrusion [7]. In [8], the study aims to design a model that deals with real intrusion detection problems in data analysis and classify network data into normal and abnormal behaviors. It proposes a multi-level hybrid intrusion detection model that uses support vector machine and extreme learning machine to improve the efficiency of detecting known and unknown attacks. A modified K-means algorithm is also proposed to build a high-quality training dataset that contributes significantly to improving the performance of classifiers. The modified K-means is used to build new small training datasets representing the entire original training dataset, significantly reduce the training time of classifiers, and improve the performance of intrusion detection system. The popular KDD Cup 1999 dataset is used to evaluate the proposed model. Compared with other methods based on the same dataset, the proposed model shows high efficiency in attack detection, and its accuracy (95.75%) is the best performance thus far [8]. In [9], The proposed work focuses on accuracy and efficiency. One way to improve performance is to use a minimal number of features to define a model in a way that it can be used to accurately discriminate normal from anomalous behavior. So the new system uses an optimized feature selection algorithm to produce the reduced set of features and high attack detection accuracy can be achieved by using a layered approach. The feature selection algorithm used in the proposed system is a multi-objective particle swarm optimization algorithm which does the feature selection effectively. The layered approach is effectively applicable to detect anomaly attack. The proposed system is tested with the benchmark KDD '99 intrusion dataset as well real-time captured data set, which outperforms other well-known methods such as the decision trees, naive Bayes and Ant Colony optimization. In [10]; the authors proposed an SVM-based intrusion detection system, which combines a hierarchical clustering algorithm, a simple feature selection procedure, and the SVM technique. The hierarchical clustering algorithm provided the SVM with fewer, abstracted, and higher-qualified training instances that are derived from the KDD Cup 1999 training set. It was able to greatly shorten the training time, but also improve the performance of resultant SVM. The simple feature selection procedure was applied to eliminate unimportant features from the training set so the obtained SVM model could classify the network traffic data more accurately. The famous KDD Cup 1999 dataset was used to evaluate the proposed system. Compared with other intrusion detection systems that are based on the same dataset, this system has been shown better performance in the detection of DoS and Probe attacks, and the best performance in overall accuracy [10]. In [11], the authors proposed a method for detecting DDOS attacks in real time at the level of the application layer. They devised a new set of tools for teaching and testing their model, derived from the absolute time interval criterion. Their method uses cuckoo, bat, and shark algorithms. As a result, the Cuckoo's Binary Clustering strategy minimizes the cost overhead of the two algorithms and increases the accuracy of prediction [12]. In [13]; an intrusion detection system called Denial of Service Intelligent Detection (DoSID) is developed. The author proposed model is the feed-forward neural network and related improvements, such as the gray area that uses the concept of distribution. The neural network is composed of two layers. The dataset used is the DARPA suite, which uses its 18 features to identify attacks. The results showed that the feed-forward neural network was successful in identifying known and unknown attacks, and the improvement of the gray area caused a significant increase in false negatives. In [14], the authors proposed an IIDDS at the System Call (SC) level using data-mining and forensic techniques. By maintaining user profiles and based on system call patterns, the system is prevented from attack and intruders. The proposed model, in contrast to the TF-IDF model, has had a better response time, accuracy, and alarm accuracy [14]. In [15], The authors have examined

whether the change in the H index can affect the destruction of the PDDOS attack. The NS2 simulator was used to generate network traffic in various scenarios using the change in traffic, pulse length and loading speed. A congestion control algorithm has been used to model PDDOS attacks. Self-similarity is used as a feature of traffic flows that are measured using the hurst parameter to detect a variety of PDDOS attacks. Self-similarity correction refers to certain features of objects that do not change with scale. They showed that in the event of an attack, the level of self-similarity increases, which results in an increment in the H parameter. Increasing self-similarity depends on the length, duration, and frequency of PDDOS attack pulses [16]. Given that the DoS attack on critical infrastructures such as government websites is a major issue, the authors proposed a cookie based accounting model in [17]. Also, they have analyzed all the accounting models including the proposed accounting model based on qualitative and quantitative results to prove the effectiveness of the proposed model. The results show that the proposed model achieves more efficiency compared to the existing model [17]. Many studies have been conducted on intrusion detection and used from the multiple machine learning algorithms, such as classification and clustering, or combining them with different ideas along with a feature selection approach. Considering the researches done in the past, the issue of reducing false alarms, as it should not have been considered, and there seems to be a gap in this area. So, in this article, we have been proposed the novel approach to resolve the gap and provide the proposed method as followings.

Table 1. An overview of researches of IDS design.

Authors (Year)	Used Algorithms	Method	Results
Hasani et al.	LGP-BA, SVM	The LGP-BA algorithm was used to feature selection and the SVM was used to categorize the acquired features.	Increased accuracy and efficiency.
Gupta and Shrivastava	BC, SVM	SVM was used to classify normal attacks and BC to enhance performance improvements in IDS.	Increased accuracy.
Kim et al.	SVM, C4.5	The combination of misuse detection and anomaly detection methods is used to detect intrusions.	Reduces the high time complexity of the training and testing processes.
Guo et al.	k-NN, k-means	K-NN and K-means algorithms are used to reduce FPR and FNR.	Detect network anomalies effectively with a low false positive rate.
Hu et al.	AdaBoost	An Intrusion Detection Algorithm is introduced based on the AdaBoost algorithm.	Low computational complexity and error rates.
Mazraeh et al.	AdaBoost, j48, IG	The main learning algorithms, SVM, Bayes Naive, and J48, have been used for feature categorization.	The superiority of the efficiency of the proposed method.
Singh et al.	OS-ELM	A technique based on the Online Sequential Extreme Learning Machine (OS-ELM) is presented.	Outperforms other published techniques in terms of accuracy, false positive rate and detection time.
Al-Yaseen et al.	SVM, ELM, k-means	A multi-level hybrid intrusion detection model is presented using a combination of K-means, SVM,	High efficiency in attack detection and its accuracy is the best performance thus far.

Authors (Year)	Used Algorithms	Method	Results
		and ELM algorithms.	
Sujitha and Kavitha	Layered MPSO	A multi-objective particle swarm optimization algorithm is used for feature selection.	The system is highly robust and efficient and can deal with real-time attacks and detect them a fast and quick response.
Hornng et al.	SVM, BIRCH	An SVM-based intrusion detection system with BIRCH algorithm is proposed.	Detects DoS and Probe attacks better than previous methods.

Types of Detection Techniques

Overview of Anomaly Detection in IDS

Anomaly detection in Intrusion Detection Systems (IDS) is a technique that identifies unusual behavior in network traffic or system activities that deviates from the established normal patterns. Unlike signature-based detection, which relies on predefined attack patterns, anomaly detection focuses on **behavioral deviations**, making it effective in detecting **zero-day attacks and novel threats**. However, a key challenge of anomaly detection is the **high false positive rate**, as legitimate but uncommon activities can sometimes be flagged as intrusions. Anomaly detection can be implemented using various techniques, including **statistical approaches and machine learning algorithms**. These techniques help define what constitutes "normal" behavior and identify outliers that may indicate malicious activity.

III. MACHINE LEARNING TECHNIQUES (FOCUS ON SVM)

Machine learning has revolutionized anomaly detection by enabling IDS to learn from data and recognize complex attack patterns. **Support Vector Machines (SVM)** is one of the most widely used machine learning algorithms in anomaly detection due to its ability to handle **high-dimensional data and nonlinear decision boundaries**.

How SVM Works in IDS:

- SVM creates a hyperplane that separates normal and anomalous data points based on labeled training data.
- It uses **kernel functions** to map input data into higher dimensions, making it easier to identify complex attack patterns.
- **One-class SVM (OCSVM)** is often used in anomaly detection, where the model is trained only on normal data and flags deviations as potential attacks.

Misuse Detection Techniques

Overview of Misuse Detection in IDS

Misuse detection, also known as **signature-based detection**, identifies intrusions by comparing network activity against a database of known attack patterns. It is highly effective in detecting **known threats** but **fails to recognize zero-day attacks or mutated malware**.

Signature-Based Detection

Signature-based IDS relies on predefined attack signatures stored in a database. These signatures can be derived from:

- **Known attack patterns** (e.g., malware signatures, brute force login attempts)
- **Packet inspection** (e.g., specific byte sequences in network packets)

Examples of signature-based IDS include **Snort and Suricata**, which use rule-based detection to match traffic against known threat indicators.

Hybrid Intrusion Detection Systems

Concept and Advantages

A **Hybrid Intrusion Detection System (HIDS)** combines **anomaly-based and misuse-based detection** to leverage the strengths of both approaches while mitigating their weaknesses.

- **Anomaly-based detection** identifies new and unknown threats.
- **Misuse-based detection** ensures high accuracy for known attacks.

By integrating both techniques, hybrid IDSs achieve **higher detection accuracy, reduced false positives, and better adaptability to evolving threats.**

INTEGRATION OF ANOMALY AND MISUSE DETECTION

Hybrid IDSs typically use a two-layered approach:

1. **Anomaly detection module:** Flags suspicious activity based on deviations from normal behavior.
2. **Misuse detection module:** Confirms if the anomaly matches known attack signatures, reducing false positives.

IV. PERFORMANCE EVALUATION

Evaluating the performance of an Intrusion Detection System (IDS) is crucial to determining its effectiveness in detecting cyber threats while minimizing false alarms. Several key metrics are commonly used for this purpose, including accuracy, precision, recall, F1-score, false positive rate (FPR), and detection rate. Accuracy measures the overall correctness of the IDS in classifying network traffic, while precision quantifies the proportion of correctly identified intrusions among all flagged instances. Recall, also known as sensitivity, assesses the ability of the IDS to detect actual threats, and the F1-score provides a balanced evaluation of both precision and recall. The false positive rate is a critical metric, as a high FPR indicates that benign activities are frequently misclassified as intrusions, leading to unnecessary security alerts. Additionally, the detection rate, or true positive rate, determines how effectively the IDS identifies malicious activities in real-time network environments.

When comparing SVM-based IDS to other techniques, it is evident that SVM offers significant advantages in handling complex attack patterns and high-dimensional data. Unlike traditional signature-based IDS, which rely on predefined attack patterns, SVM can generalize from training data to detect novel threats. Compared to other machine learning algorithms, such as Decision Trees and k-Nearest Neighbors (k-NN), SVM often demonstrates superior classification accuracy, especially when dealing with imbalanced datasets. However, its computational complexity can be a challenge, particularly in large-scale network environments where real-time detection is required. Deep learning-based IDS, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have emerged as strong competitors, offering higher adaptability but requiring extensive computational resources and large labeled datasets for training. The challenge in IDS performance evaluation lies in selecting appropriate datasets, handling class imbalances, and ensuring that evaluation metrics reflect real-world attack scenarios. Publicly available datasets like NSL-KDD, CIC-IDS2017, and UNSW-NB15 are widely used for benchmarking, but they often fail to capture the complexity of modern cyber threats.

V. APPLICATIONS OF IDS

Real-world applications of SVM-based hybrid IDS have demonstrated their effectiveness in securing enterprise networks, cloud environments, and industrial control systems. Organizations deploy hybrid IDS solutions to monitor network traffic, detect anomalies, and prevent cyberattacks in real time. In cloud security, SVM-based IDS is used to detect unauthorized access, data breaches, and distributed denial-of-service (DDoS) attacks. Industrial networks, such as those in critical infrastructure and smart grids, benefit from hybrid IDS solutions to identify malicious activities while minimizing operational disruptions. Case studies highlight the effectiveness of SVM-based IDS in improving cybersecurity resilience. For example, research studies implementing SVM in hybrid IDS architectures have reported higher detection accuracy compared to standalone IDS solutions. One study integrated SVM with deep learning techniques, achieving over 98% detection accuracy on benchmark datasets while reducing false positives. Another implementation enhanced traditional IDS tools like Snort by incorporating SVM classifiers to detect zero-day attacks, demonstrating a significant improvement in threat detection capabilities. However, challenges in deployment remain, including high computational costs, difficulty in

real-time processing of large network traffic volumes, and adversarial attacks that attempt to evade detection by modifying attack patterns.

VI. CONCLUSION AND FUTURE WORK

The future of SVM-based hybrid IDS is shaped by emerging trends in artificial intelligence and cybersecurity. One promising direction is the integration of deep learning and reinforcement learning techniques to enhance IDS adaptability. Federated learning is also gaining traction, allowing multiple IDS nodes to collaborate and improve detection performance without sharing raw data, preserving privacy. Additionally, research is focused on developing lightweight IDS solutions optimized for edge computing and Internet of Things (IoT) environments. Despite these advancements, several research gaps and challenges remain, including the need for better feature selection methods, improved handling of adversarial attacks, and reducing the computational burden of SVM training and classification. Future prospects for SVM-based hybrid IDS include the development of automated and self-learning systems that continuously evolve to counter new attack vectors, ultimately strengthening network security in dynamic and high-threat environments.

REFERENCES

- [1] S. R. Hasani, Z. A. Othman, and S. M. M. Kahaki, "HYBRID FEATURE SELECTION ALGORITHM FOR INTRUSION DETECTION SYSTEM," *J. Comput. Sci.*, vol. 10, no. 6, pp. 1015–1025, Jan. 2021, doi: 10.3844/jcssp.2014.1015.1025.
- [2] M. Gupta and S. K. Shrivastava, "Intrusion Detection System based on SVM and Bee Colony," *Int. J. Comput. Appl.*, vol. 111, no. 10, pp. 27–32, 2022, doi: 10.5120/19576-1377.
- [3] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Syst. Appl.*, vol. 41, no. 4, Part 2, pp. 1690–1700, 2022, doi: <https://doi.org/10.1016/j.eswa.2013.08.066>.
- [4] C. Guo, Y. Ping, N. Liu, and S.-S. Luo, "A two-level hybrid approach for intrusion detection," *Neurocomputing*, vol. 214, pp. 391–400, 2022, doi: <https://doi.org/10.1016/j.neucom.2016.06.021>.
- [5] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," *IEEE Trans. Syst. Man, Cybern. Part B*, vol. 38, no. 2, pp. 577–583, 2023, doi: 10.1109/TSMCB.2007.914695.
- [6] "View of Intrusion detection system with decision tree and combine method algorithm.pdf."
- [7] R. Singh, H. Kumar, and R. K. Singla, "An intrusion detection system using network traffic profiling and online sequential extreme learning machine," *Expert Syst. Appl.*, vol. 42, no. 22, pp. 8609–8624, 2021, doi: <https://doi.org/10.1016/j.eswa.2015.07.015>.
- [8] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Syst. Appl.*, vol. 67, pp. 296–303, 2022, doi: <https://doi.org/10.1016/j.eswa.2016.09.041>.
- [9] B. Ben Sujitha and V. Kavitha, "Layered approach for intrusion detection using multiobjective particle swarm optimization," *Int. J. Appl. Eng. Res.*, vol. 10, no. 12, pp. 31999–32014, 2023.
- [10] S.-J. Horng *et al.*, "A novel intrusion detection system based on hierarchical clustering and support vector machines," *Expert Syst. Appl.*, vol. 38, no. 1, pp. 306–313, 2023, doi: <https://doi.org/10.1016/j.eswa.2010.06.066>
- [11] Kumar, Vinod, and Om Prakash Sangwan. "Signature based intrusion detection system using SNORT." *International Journal of Computer Applications & Information Technology* 1.3 (2012): 35-41.
- [12] Mehta, Vishal, et al. "Threat prediction using honeypot and machine learning." 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE). IEEE, 2015.
- [13] Haas, Steffen, Robin Sommer, and Mathias Fischer. "Zeek-osquery: Host-network correlation for advanced monitoring and intrusion detection." *ICT Systems Security and Privacy Protection: 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21–23, 2020, Proceedings 35*. Springer International Publishing, 2020.
- [14] R. Lehti, P. Virolainen: AIDE (Advanced Intrusion Detection Environment), Web ref: <http://www.cs.tut.fi/~rammer/aide.html>
- [15] Kim, Gene H., and Eugene H. Spafford. "Experiences with tripwire: Using integrity checkers for

intrusion detection." (1994).

[16] Lenard, Teri, and Roland Bolboaca. "A statefull firewall and intrusion detection system enforced with secure logging for controller area network." European Interdisciplinary Cybersecurity Conference. 2021.

